A reversible transform is first applied so that inter-word intervals become exclusively comprised of odd numbers of blank characters. By means of a secret key, the complete transformed original text is then split in two pseudo-random, non contiguous subsets of intervals, and an authentication pattern is merged into first subset by adding inter-word blank characters. A blurring pattern is computed which further modifies the number of blank characters so as to hide the authentication pattern. A second subset is blurred too, before subsets are recombined to obtain a marked text susceptible of authentication.

A method of authenticating a received text document which has been marked according to the above-noted method is also disclosed.

The present invention also embodies a method which permits a text document to be authenticated while an authentication pattern is imbedded, and deeply hidden, into the text document itself.

Distinctive Features of the Present Invention

The invention, while being based on the principle of inserting a number of extra blanks on inter-words intervals of a text document (similar to the "open space methods" cited by Bender, et al.), has the following distinctive features, absent in the prior art:

-- The encoding method is randomized in such a way that code breakers see their job much complicated, not being able to determine which ones of the blanks intervals present in the coded text, are really holding the encoded data.

Only the authorized recipient may restore the exact original format, including the numbers of inter-word blank characters, of the original document. --

The Examiner has rejected the claims pending in this case under 35 U.S.C. §103(a) in view of A) Aikawa, et al.: US 6,606,385: *Data Encrypting/Decrypting Conversion Methods and Apparatuses and Data Communication System Adopting the Same,* and Aikawa, et al. in view of B) Bender et al.: *Techniques for Data Hiding*, IBM Systems Journal, Vol. 35, Nos. 3&4, 1996. The Examiner is requested to reconsider the rejections because the system of the present invention is totally different from the systems disclosed in the cited references, alone or in combination.

The fundamental differences between the references cited above, and the instant application are set forth in the following paragraphs which will be referred to in the specific responses to the Examiner's rejections of the claims.

1) Different Subject Matter, Systems and Methods

The apparatus (and method) described in Aikawa et al. relates to an encryption/decription system, which takes a plain text and generates an encrypted text (*unreadable to everyone except by the recipient*), or *decrypts a received enciphered text into a plain text.*

More specifically, Aikawa et al. deals with the subject of encryption and means for encoding data using a cryptographic cipher producing encrypted data that can be read (i.e., decrypted) only by an authorized entity.

To that aim, Aikawa et al. discloses a method and apparatus implementing an algorithm (a variant of the RC5 encryption algorithm) which is used to scramble data converting input data into ciphertext which makes it unreadable to everyone except the recipient. Further, Aikawa et al. deals with decryption, since the reference discloses a method and apparatus implementing an algorithm to convert ciphertext (encrypted data) into plaintext.

The present invention deals with a totally different system comprising the authentication of text documents. It is intended to guarantee and to validate that a document that was signed has not been altered, by providing means for generating, from a secret-key and the original text document, a signature or MAC (message authentication code) which is encoded and further

hidden in the original document. The present invention modifies (i.e., marks), according to disclosed algorithms, the distribution of inter-word blank characters of an original (plain) text, thus only affecting the format of the authenticated document that is transmitted to the recipient, but not to the readability of the content. This is due to the fact that the authenticated (i.e., marked) text is transmitted as a plain (i.e., non encrypted) text.

Only an authorized recipient, using the same secret-key used by the sender, is able to verify from the received text document, its authenticity. Thus only an authorized recipient is able to recover the format of the original document. This is done by reversing the transformations applied by the sender on the distribution of inter word blank characters for marking the original text document.

Applicants submit also that the method and apparatus disclosed by Aikawa et al. are directed to totally different and unrelated methods from the system claimed by Applicants for marking an original text document and for authenticating a text document marked accordingly, as claimed in Claims 1 and 2 of the instant invention.

Specifically, Claim 2 of the present invention relates to a method for authenticating (i.e., validating as authentic, or rejecting as fake) a received text document that has been previously "marked" (by the sender) utilizing the method of "marking an original text document" (i.e., of altering the numbers of blank characters on the inter-word intervals of the original plain text document) that is disclosed in Claim 1. Remainder claims 3 - 8 of the present invention are dependent claims and accordingly are allowable. Observe that the essence of Aikawa et al. refer to *"an encrypting conversion apparatus"* or to a *"decrypting conversion apparatus"*.

For the people skilled in the art, "encryption" and "authentication" of electronic documents are quite different subjects. Accordingly, totally different methods and techniques must be applied for each.

2) Different Mechanisms of Processing Text Documents:

Not only are the subject matters of Aikawa et al. reference and the present invention totally different, but also the methods used for processing documents are different (i.e., of transforming an input text document into another output document).

By way of example, the authentication method on the Claim 2 of the instant application is different from the encryption or decryption method of Aikawa et al. Even when Aikawa et al. utilize "*a module for dividing inputted plain-text data into first data and second data*", this procedure is totally different from the step in Claim 2 of *"splitting said marked text document into a first subset and a second subset of said words including the trailing said inter-word intervals of said words."*

Note in Aikawa et al., for the purposes of encrypting a "plain text" *(inputted plain-text data*), the input text (see item (101) in Figures 1, 2, 13) is processed as contiguous blocks of 64 bits. Observe also, how in Aikawa et al. the "encryption text" (see item (105) in Figure 12), is a block of 64 bits applied as the input to a "decryption unit" (401).

There is a difference in the above-mentioned way of processing input text as taught by Aikawa et al. and the processing disclosed in Applicants' invention, as is described on page 7 of the instant application and is illustrated on the Figure 2. The specific paragraph is set forth as follows:

FIG. 2 shows a function G [200], needed to carry out the invention, which can be implemented in many ways from techniques and methods well known by those skilled in the art. Irrespective of the way function G is actually implemented it is assumed to be able to generate an output S [205] which is made dependent upon three types of entries. First, S is made dependent upon an input text [220], like the ones shown in FIG. 1. Second, output S must also depend on a key [230], shared by the parties involved in the authentication process. Third, of a set of parameters [210], aimed at conditioning the way function G must process input text and key especially, specifying what type and format of output S are expected in a particular instance of the function. As an example of the way function G is used by the invention, canonical form of the text already shown in FIG. 1 [220], assumed to be ASCII coded, is the input text. Key is e.g., an alphanumeric text string [230] that must be kept secret. Then, parameter [210] may be set to instruct function G to produce for instance, a string of 23 binary bits [215]. Those skilled in the art will recognize that function G, such as described here above, could be implemented, for example, from a one-way

hash function aimed at producing a unique digest of the input text and secret key, also made dependent of input parameters, such as the number of expected bits so that output S can be tailored to fit in any particular step of the invention described in the following figures. One-way hash functions, which carry many other names like compression function, message digest, have received a considerable attention and are central to modern cryptography. A good review of this subject can be found in `Applied Cryptography` a book authored by Bruce Schneier and published by John Wiley & Sons, 2nd edition, 1996. What is specific in the hash function needed to carry out the invention, with respect to the general description that exists in the here above book and in the abundant literature on the subject, is that it must accept input parameters on top of the standard input text and key especially, to allow the size of the output to be tailored to fit a particular instance of the function. Although this is different of standard hash functions, which generally produce a fixed-size digest of a keyed-text, this does not raise any outstanding problem to those skilled in the art to devise such a function either, as suggested above, from a standard hash function or through any alternate method that would better fit in a particular implementation of the invention."

In particular, note in Figure 2 of the instant application publication how function G serially receives a complete input text (220) (non limited to a block of 64 bits, as Aikawa, et al.), and generates a pseudo-random binary string S, depending on a secret key (230) and parameters (210), to allow the size of the output to be tailored to fit a particular instance of the function. By way of illustration, given a plain text having 524 inter word intervals (i.e., 523 words), Applicants' system generates from this text and a secret-key, a pseudo-random string S of 524 bits.

Thus, it becomes evident that the way text is processed by the system of the instant invention is quite different from that described on Aikawa et al., wherein the input text, independently of the number or words (i.e., text length), is split in fixed-length blocks of 64 bits (8 bites) which are independently processed (i.e., encrypted/decrypted).

Therefore, not only the system and method of Aikawa et al. and that of our invention are totally different from the functional point of view (i.e., for the different intended functions of both systems), but also from the architectural and operational points of view.

3) Different Mechanisms of Splitting Text Documents:

It should be noted that even when Aikawa et al. apply a technique for splitting blocks of text into portions (named: L[N] and R[N]), this technique has nothing in common with the technique for splitting a full text document that is disclosed in the present invention.

In fact, in Aikawa et al. (item (101) in Figures 1, 2, 13) for the purposes of encryption, the input "plain text" *(inputted plain-text data*), is processed as a deterministic sequence contiguous blocks of 64 bits. Also (item (105) in Figure 12), how in Aikawa et al. the "encryption text" is a block of 64 bits applied as the input to a "decryption unit" (401). Moreover in Aikawa et al. , apart from splitting the input text for processing as a fixed sequence of contiguous blocks of 64 bits, each 64 bits block is also deterministically split into two fixed sub-blocks of 32 bits each (left and right), denoted respectively: L[N] and R[N].

By example, considering text splitting steps recited on the authentication method subject of the Claim 2 of the present invention, the above specification of Aikawa has no relevance to the use of the function G illustrated in the Figure 2 of the instant application which generates a pseudo-random binary string S (215) having as many bits as the number of inter word-blank characters in the input text (220) for the purpose of splitting a text into two "sub-text" portions. This process is clearly illustrated in Figure 5 and the corresponding description in the examples in the paragraphs on page 10 of the instant application publication which discloses:

FIG. 5 focuses mainly on step [310] also referring to steps [302] and [307] of FIG. 3 from where text [500] is split. Although many alternate equivalent ways are possible for these steps function G, described in FIG. 2, is used too in a preferred embodiment of the invention. That is, using the canonical form of text and the shared secret-key as inputs, function G is set to generate a split binary vector [510] fitting the number of inter-word text intervals.

It is worth noting here that whichever method is actually used to split a text it must provide, for a given combination of `ctext` and secret-key, a unique manner of splitting the text so that the recipient of an authenticated text marked according to the method of the invention will be able upon reception to obtain the same split. In practice, this requires that, in the preferred embodiment of the invention which uses function G previously described, that input parameters to

be used be agreed upon in advance (or the method of unambiguously determining them) between the sender and the receiver.

Then, using the split binary vector [510], words and associated trailing blanks, corresponding to the asserted bit of the vector are said to belong to a subset e.g., `stext1` [520] while those corresponding to non asserted bits are said to belong to the other subset `stext2` [530]. As already mentioned above, split binary vector [510] must be remembered to allow proper recombination of subsets as described at step [340] of FIG. 3.

Thus, even when Aikawa et al. utilizes "*a module for dividing inputted plain-text data into first data and second data*", this procedure has no similarity to the steps on Claims 1 and 2 of "*splitting said original (or marked text document) into a first subset and a second subset of said words including the trailing said inter-word intervals of said words*".

While in the present invention a complete input text (independently of its size) is pseudo randomly split into two "sub-text" (non contiguous) portions, Aikawa et al. splits the input text for processing as a (fixed) sequence of contiguous blocks of 64 bits, where each 64 bits block is itself split into two contiguous sub-blocks of 32 bits each (left and right), denoted respectively: L[N] and R[N].

Therefore, not only are the system and method of Aikawa et al. and that of the present invention functionally and operatively different, but the technical procedures applied, such as how input text is partitioned for processing, are also radically different.

4) The Use of the Canonical Form of a Text Document:

The present invention introduces and uses the concept of "canonical form" of a text document. Claim 3 of the instant application covers this feature and provides:

-- **3.** The method ... wherein splitting steps includes the preliminary steps of:

generating a canonical form of a text document;

computing from said canonical form of said text document and said secret-key, a splitting pattern that fits the number of said intervals of said text document;

thereby, allowing to split and to recombine said text document on the basis of asserted and non-asserted bits of said splitting pattern.--

In the present invention, the "canonical form" of a text document is defined for the purpose of computing (in combination with a secret-key) *"a splitting pattern that fits the number of said intervals of said text document."* Observe how this "splitting pattern" is randomized by the use of the secret-key.

Applicants point out that the disclosure (and the use) of a "canonical form" is absent in Aikawa et al. wherein a text document is split an processed in fixed contiguous blocks of fixed length of 64 bits, each one being itself split it two sub-blocks L[N] and R[N], of 32 bits.

Claim 5 of the instant invention defines how to generate the "canonical form" of an input text.

Claim 5 states:

- - **5.** The method... wherein said canonical form is obtained in stripping all blank characters, in excess of one, off said inter-word intervals. - -

In this respect, Applicants clarify that, - quite different from the opinion of the Examiner -, the use of the "canonical form" of a text document has <u>not</u> been employed in the present invention for the purpose of compressing data to be transmitted.

It is as stated in Claims 1, 2 and 3 of the application:

On Claim 1, for:

> computing, from said canonical form of said first subset and said secret-key, a blurring pattern that fits the number of said intervals of said first subset;
>
> computing, from said canonical form of said second subset and said secret-key, a blurring pattern that fits the number of said intervals of said second subset;

On Claim 2, for :

computing, from said canonical form of said first subset and a secret-key, a blurring pattern that fits the number of said intervals of said first subset;

and for...

Ÿ computing, from said canonical form of said second subset and said secret-key, a blurring pattern that fits the number of said intervals of said second subset;

On Claim 3, for:

computing, from said canonical form of said text document and said secret-key, a splitting pattern that fits the number of said intervals of said text document;

Thus, Applicants respectfully point out to the Examiner that the purpose and use of "canonical forms" in the present invention is to generate "authentication patterns, blurring patterns and splitting patterns", not to compress data to be transmitted. Applicants therefore disagree with the following assertions of the Examiner in the Detailed Action, where it is stated:

"*It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the canonical form of each subset of data because this compress the data and hence reduces the amount of overhead being sent when the watermarked text document is transmitted from a sender to a receiver.*"

and:

"It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bender within the system of Aikawa et al because stripping all the blank characters in excess of one character manipulates the white space manipulation to achieve data compression. This saves overhead during data transmission".

Quite differently from the use expressed by the Examiner, the "canonical form" of a text is a local transformation of a text document (or a portion of it), intended for computation purposes; it is not being transmitted in the "canonical form" from the sender to the receiver.

Since the "canonical form" of a text is created *"by stripping all blank characters, in excess of one, off said inter-word intervals"*, it is therefore independent of the original distribution on inter-words blank characters (i.e., is a "canonical" representation of the text), being only dependent on the information content (i.e., on the normalized sequence of words of the text).

Moreover, from Claims 4 and 6 of the instant invention:

- - 4. The method according to ... wherein said authentication pattern, said blurring pattern and said splitting pattern are binary vectors comprised of a number of bits matching the number of corresponding said inter-word intervals. - -

- - 6 The method ... wherein modifying steps include:
in the positions corresponding to the asserted bits of said blurring pattern adding one blank character if said inter-word intervals are comprised of an odd number of said blank character;
removing one blank character if said inter-word intervals are comprised of an even number of said blank characters. - -

Applicants point out that the purpose and use of "canonical forms" in the invention is to generate *"authentication patterns, blurring patterns and splitting patterns"* as *"binary vectors comprised of a number of bits matching the number of corresponding said inter-word intervals"* for the purposes of *"adding or removing blank characters"*. The result of this transformation consisting on *"adding or removing blank characters"* is not equivalent to compressing information, contrary to the opinion of the Examiner.

Applicants submit that the present invention is different from Aikawa et al., not only from the perspective of that different subject matters, but also in that the architecture, functions, algorithms and operations of the system and method described in the instant application are absolutely different from those of Aikawa et al.

Therefore, Applicants respectfully reject as improper the Examiner's assertion that, based upon the teachings about data encrypting/decrypting methods and apparatuses described by Aikawa et al., a person skilled in the art at the time of the invention would be able to devise the inventive solution disclosed by Applicants with the combination of technical elements applied in the methods disclosed by the instant invention for reversibly marking text documents for authentication.

The technical elements, idea and/or principles, in Aikawa et al., cannot be applied to solve the problem posed with respect to the objects of the present invention.

Comparative Analysis of the Instant Application and Bender et al., "*Techniques for Data Hiding*", Bender et al., IBM Systems Journal, Vol. 35, Nos. 3&4, 1996

The Examiner's primary source for the rejections in this reference is the "Open Space Methods" described on pages 332 and 333 of Bender et al.

Applicants respectfully point out to the Examiner that on page 3 of the instant application Applicants refer to Bender et al., and particularly to the different techniques proposed in this reference for hiding data on text documents. After analyzing those techniques, particularly the "Open Space Methods" from Bender et al, Applicants stated that the solutions proposed in this prior art for hiding data on text documents (e.g., a MAC or authentication signature) presented some important drawbacks which prevented the Bender et al. solutions to be applied for the purposes of the present invention. Basically, Bender et al. describe three different "open space methods", all of them based on using blank spaces to encode data. These methods manipulate the number of blanks at the "*end-of-sentences*", at the "*end-of-lines*" or "*between-the-words.*"

1) The first "open space" method of Bender, et al. encodes a binary message into a text by "sequentially" placing either one or two spaces after each terminating character (e.g., a period or a semicolon); where, for example, a single space encodes a "**0**" and two spaces encodes a "**1**". This method of Bender, et al. is inefficient, since it requires a large text to encode a few bits, its ability to encode depends on the structure of the text and, what is even worse, due to the fact that the "hidden" information is sequentially encoded in the text, it is a very easy task for an adversary to recover the encoded ("hidden") information from a soft-copy of the text file.

2) The second "open space method" of Bender, et al. consists of inserting additional spaces at the end of lines. For example, two additional spaces encode one bit per line, four encode two, eight encode three, etc., thus increasing considerably the amount of information that can be encoded over the previous method. Due also to the fact that the hidden information is sequentially encoded on successive end-of-line positions, the system provides a very easy task for an attacker to recover the encoded information from soft-copy texts.

3) The third "open space" method of Bender, et al. requires right-justification of the text and consists in encoding data by controlling the number of spaces between words on this right-formatted text. For example, one space between words is interpreted as a "**0**", two spaces is interpreted as a "**1**", thus enabling this method to encode several bits per line. To unambiguously determine the locations where inter-word spaces encode hidden data and where they do not, Manchester-like encoding procedures are used. In such a scheme, groups of bits are encoded in sets of two and interpreted as follows: "**01**" is "**1**", "**10**" is "**0**" and "**00**" or "**11**" is a null (no information). Although this "open space" method has a greater capability for hiding information in a text, it is still a sequential method, thus making it an easy task to identify and recover encoded information by analysis of the soft-copy text format.

Thus, a major drawback of "open space" text data hiding techniques described in Bender et al. is that, in one form or another, all them present many "open doors" for a skilled adversary hacker to recover the encoded information from soft-copies of original texts, even by means of simple personal computers, and by using very simple, widely available software tools (e.g., byte-file editors or Norton utilities). Therefore, none of these data hiding methods can be used effectively as a means for improving the security of secret key authentication methods, aimed for using a technique of hiding integrity information generated on a text, such as a MAC value, into the text itself.

From the analysis on the security concerns of modern secret key text authentication methods and the limitations on the security of different text data hiding techniques proposed so far (including "open space" methods described by Bender et al.), Applicants concluded that there was a need for a new text data hiding method that could hide the integrity information generated on a text into the text itself, in such a form as to make impractical or impossible, the task of locating, identifying and recovering the integrity information encoded into the text.

Particularly, from this analysis Applicants concluded that there was a need for new "open space" methods, able to satisfy the requirements of a system aimed for improving security.

A first requirement for a new text integrity encoding and data hiding method to be embodied in the present invention is that the novel system and method should be deterministic only to the authenticator and to the verifier, while it must appear to any adversary as being non-deterministic and non-sequential. Applicants invention has done this.

More specifically, Applicants considered essential in their invention that a new text data hiding method should be an "random open space" method that would hide the integrity information to be encoded into texts on some secret-key determined, non-sequential positions of the blanks intervals between text words. None of those requirements are met by the "open space" methods described by Bender et al.

No less important, a second requirement for the new data hiding method in Applicants' invention has been to enable the receiver not only to recover, decode and verify the hidden integrity information, but to enable the receiver also to recover the original format of a text from the received authenticated (i.e., "marked") text.

Therefore, with the aim of improving the Bender, et al. prior art, Applicants formulated the following objectives of their invention:

"*...Therefore it is a broad object of the invention to provide a method to merge the information necessary to authenticate a text document, into the body of the document itself, under the form of extra inter-word blanks. It is another object of the invention to permit that the recipient of the document be able to restore exactly the format, including the number of blanks, of the original text. It is still another object of the invention to merge the extra blanks, actually carrying the authentication data, with dummy blanks so as to even confuse more an attacker...*"

The present invention, while being similar to Bender et al. in that it provides an "open space" method to merge, under the form of extra inter-word blanks, the information necessary to authenticate a text document into the body of the document itself is different to all "open spaces"

methods disclosed in the prior art, in that the method:

- - Merges the extra blanks, actually carrying the authentication data, with dummy blanks so as to confuse an attacker; - - and

- - Permits the recipient of the document to restore exactly the format, including the number of blanks, of the original text. - -

Thus, Applicants respectfully reject the suggestion that, in the light of the teachings about "open space" methods described by Bender et al., a person skilled in the art at the time of the invention would be able to devise the inventive solution and the combination of technical elements applied in the instant invention for reversibly marking text documents for authentication.

Therefore, based upon the analysis discussed hereinabove relating to Aikawa et al. and Bender et al., Applicants respectfully disagree with the assertions of the Examiner in that one of ordinary skill in the art at the time of the invention, using the teachings of Bender et al. and Aikawa et al., would be able to devise the method of the present invention.

Applicants Specific Response to Claim Rejections

1. In the Detailed Action, the Examiner rejects Claims 2 - 4 under 35 U.S.C. 103(a) as being unpatentable over Aikawa et al (US 6,606,385 B1).

In his rejection, the Examiner considers that Applicants claim language which states:

"*...splitting said marked text document into a first subset and a second subset of said words including the trailing said inter-word intervals of said words; and, over said first subset: generating canonical form of said first subset; computing, from said canonical form of said first subset and a secret-key, a blurring pattern that fits the number of said intervals of said first subset; erasing modifications brought to the numbers of said inter-word blank characters per said blurring pattern; extracting an authentication pattern thereby, obtaining in all said inter-word intervals odd numbers of blank characters; and, over said second subset: generating canonical form of said second subset; computing, from said canonical form of said second subset and said secret-key, a blurring pattern that fits the number of said intervals of said second subset; erasing modifications brought to the numbers of said inter-word blank characters per said blurring*

pattern thereby, obtaining in all said inter-word intervals odd numbers of blank characters..."; ("the Limitation")

is met in Aikawa, et al. at column 2, lines 42-65 which states:

Thus, there is provided according to an aspect of the present invention an encrypting conversion apparatus which receives as inputs thereto at least one key and plain-text data to thereby output encrypted text data, which apparatus can be implemented in hardware fashion or software fashion and includes a cyclic shift processing module for determining a shift number on the basis of data for determining a shift number selecting sequence, a module for dividing inputted plain-text data into first data and second data and setting the first data as data L[1] while setting the second data as data R[1], at least one stage of an encrypting conversion processing module for receiving as inputs thereto data L[N] and R[N] to thereby output data L[N+1] and data R[N+1], wherein the encrypting conversion processing module is so arranged as to perform at least once for the data L[N] a conversion processing by using the key and a cyclic shift processing by means of the cyclic shift processing module, respectively, to thereby generate data X and wherein a value derived from arithmetic operation of the data R[N] and the data X is set as the data L[N+1] while the data L[N] being set as the data R[N+1], and a module for outputting a combination of two output data from a final stage of the encrypting conversion processing module as an encrypted text.

From Applicants' analysis of Aikawa et al. as provided in paragraphs 1 - 4 set forth above and specifically the analysis of the above-cited excerpt by the Examiner, Applicants cannot identify any similarity or relevance of the "encrypting conversion apparatus" described by Aikawa et al. to the system and method of the present invention. Applicants therefore, respectfully disagree with the Examiner's rejection.

The Examiner considers that the Limitation is also met by Aikawa, et al. at column 13, lines 13-26 which states:

Referring to the figure, a contents provider 1401 registers copyright information at a copyright managing facility 1418 to obtain contents identification information (IDA) 1402. The contents identification information (IDA) 1402 is embedded into the contents data 1403 by resorting to an electronic transparentizing technique (or so-called digital watermarking technique) which allows the identification information or the like to be contained in digital data in a hidden state, whereby package contents 1404 is finished. FIG. 19 is a schematic view illustrating the contents data contained in the package contents 1404, wherein the contents identification information (IDA) 1402 is embedded as an electronic transparent information.

The excerpt cited above refers to a technique for hiding data (the IDA) on a format different from a plain text document (as for example, videos, music songs or digital pictures). Observe that, from the same reference cited by the Examiner (see Bender et al.), this watermarking technique cannot be applied for hiding data on plain text documents, as is the case of the present invention. In fact, according to Bender et al., page 332, see *Data hiding in text* section, soft-copy texts are in many respects the most difficult places to hide (i.e., to steganographically hide) data. This is due mainly to the relatively small quantity of redundant information in a text file, as compared with an image or sound record. Although one can often imperceptibly modify a picture, this is not the case for a soft-copy text, where a single modification to the text, like an extra letter or period, can be noticed even by a casual reader. Hence, the argument on the cited paragraph can not be applied to the instant invention. Therefore, Applicants respectfully oppose to this argument by the Examiner.

The Examiner contends that Applicants' language:

"*recombining said first subset and said second subset; applying a reverse transform thus, retrieving said original text document; computing, from retrieved said original text document and said secret-key, an authentication pattern that fits the number of said intervals of retrieved said original text document; comparing extracted said authentication pattern and computed said authentication pattern; if matching exactly: accepting said marked text document as authentic; if not: rejecting said marked text document as fake*"

is met by Aikawa, et al. at column 3, lines 11-33, which provides:

Further, according to another aspect of the present invention, there is provided a decrypting conversion apparatus which receives as inputs thereto at least one key and encrypted text data to thereby output plain-text data, which apparatus can be implemented hardware-wise or softwarewise and includes a cyclic shift processing module for determining a shift number on the basis of data for determining a shift number selecting sequence, a module for dividing inputted encrypted text data into first data and second data and setting the first data as data L[1] while setting the second data as data R[1], at least one stage of a decrypting conversion module for receiving as inputs thereto data L[N] and R[N] to thereby output data L[N+1] and data R[N+1], wherein the decrypting conversion module is so arranged as to perform at least once for the data R[N] a conversion processing by using the key and a cyclic shift processing by means of the cyclic shift processing module, respectively, to thereby generate data X and wherein a value derived from arithmetic operation of the data L[N] and the data X is set as the data R[N+1] while the data R[N] being set as the data L[N+1], and a module for outputting a combination of two output data from final stage of the encrypting conversion module as a plain-text.

From the conclusions reached in the analysis of Aikawa et al. (see arguments presented in paragraphs 1, 2, 3, 4), Applicants cannot identify any similarity or relevance of the "decrypting conversion apparatus" described by Aikawa et al. and the system and method of the present invention.

The Examiner considers that the Limitation is also met by Aikawa at column 13, lines 43-47 which states:

On the other hand, in the personal computer (C) 1411 which receives the contents data from the home-use-destined electric/electronic equipment (B) 1405, the encrypted data is decrypted by a decryption apparatus 1412 according to the invention by using key data (K) 1415.

As was discussed in Applicants' analysis of Aikawa et al. (see particularly paragraph 1), Applicants again emphasize that in the present invention there is no encryption or decryption process, since text documents are transmitted and received as plain (i.e., non-encrypted) text documents. Therefore, Applicants respectfully refuse to acknowledge any analogy of the system and method of the present invention and the prior art systems cited by the Examiner relating to a system implementing encryption and decryption processes.

The Examiner considers that the Limitation set forth above is also met by Aikawa, et al. at column 14, lines 2-10 which states:

Upon detection of the data not decrypted, the contents identification information IDA contained in the data is matched with the information contained in a copyright information managing database 1420. When it is decided as the result of the matching that the data of concern is unauthorized copy, the copyright managing facility 1418 traces the latter back to the origin by making use of the user identification information and can impose penalty.

As noted above, in the present invention there is no decryption process, since text documents are transmitted and received as plain (i.e., non-encrypted) text documents.

Also, the above paragraph of Aikawa et al. refers to a technique for extracting data (the IDA) that has been encoded and hidden on a format different from a plain text document (as for example, videos, music songs or digital pictures). Observe that, from the Bender, et al. reference cited by the Examiner, this watermarking technique cannot be applied for hiding data on plain

text documents, as is the case in the operative environment of the present invention. In fact, according to Bender et al., page 332, *Data Hiding in Text* section, soft-copy texts are in many respects the most difficult places to hide (i.e., to steganographically hide) data. This is due mainly to the relatively small quantity of redundant information in a text file, as compared with an image or sound record. Although one can often imperceptibly modify a picture, this is not the case for a soft-copy text, where a single modification to the text, like an extra letter or period, can be noticed even by a casual reader. Hence, the argument on the cited paragraph from Aikawa, et al. can not be applied to the present invention. Therefore, Applicants respectfully disagree with the cited argument by the Examiner.

Referring further to the above Limitation, the Examiner states that :

"The encryption of data represents the blurring pattern creation"

As noted above, in the present invention there is absolutely no encryption process or encryption apparatus involved; thus Applicants cannot acknowledge as accurate the above-cited contention put forward by the Examiner. The suggestion that the encryption apparatus of Aikawa et al. could be (hypothetically) applied in some non demonstrated form for generating a "blurring pattern" for the purposes intended by the instant invention is speculative, since the apparatus (and algorithms implemented) utilized in the instant invention for this generating "blurring patterns" (see function G on Figure 2 of the instant application) is quite different from the apparatus described by Aikawa et al. Such apparatus is aimed to the specific tasks of encryption and decryption, not authentication of plain text documents. See in this respect, paragraph 1 of the analysis of Aikawa et al. set forth above.

In the rejection relating to the Limitation, the Examiner states that :

"It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the canonical form of each subset of data because this compress the data and hence reduces the amount of overhead being sent when the watermarked text document is transmitted from a sender to a receiver".

As demonstrated on Applicants analysis of Aikawa et al. (see especially paragraph 4 above), on the system of the present invention "canonical forms" of texts are purposely and exclusively used to generate "authentication patterns, blurring patterns and splitting patterns", not

to compress the data to be transmitted. (Emphasis Added) In fact, in the present invention the "canonical form" of a text is only used for computation purposes, and is never transmitted. Thus, Applicants respectfully reject this assertion of the Examiner.

2) With respect to Claim 3 which states:

- -**3.** The method of anyone of the previous claims wherein splitting steps includes the preliminary steps of:

generating a canonical form of a text document;

computing, from said canonical form of said text document and said secret-key, a splitting pattern that fits the number of said intervals of said text document;

thereby, allowing to split and to recombine said text document on the basis of asserted and non-asserted bits of said splitting pattern. - -

The Examiner considers that the limitation of:

"*splitting steps includes the preliminary steps of: generating a canonical form of a text document; computing, from said canonical form of said text document and said secret-key, a splitting pattern that fits the number of said intervals of said text document; thereby, allowing to split and to recombine said text document on the basis of asserted and non-asserted bits of said splitting pattern*" is met by Aikawa, et al. at column 2, lines 42-65, which states:

Thus, there is provided according to an aspect of the present invention an encrypting conversion apparatus which receives as inputs thereto at least one key and plain-text data to thereby output encrypted text data, which apparatus can be implemented in hardware fashion or software fashion and includes a cyclic shift processing module for determining a shift number on the basis of data for determining a shift number selecting sequence, a module for dividing inputted plain-text data into first data and second data and setting the first data as data L[1] while setting the second data as data R[1], at least one stage of an encrypting conversion processing module for receiving as inputs thereto data L[N] and R[N] to thereby output data

L[N+1] and data R[N+1], wherein the encrypting conversion processing module is so arranged as to perform at least once for the data L[N] a conversion processing by using the key and a cyclic shift processing by means of the cyclic shift processing module, respectively, to thereby generate data X and wherein a value derived from arithmetic operation of the data R[N] and the data X is set as the data L[N+1] while the data L[N] being set as the data R[N+1], and a module for outputting a combination of two output data from a final stage of the encrypting conversion processing module as an encrypted text.

From Applicants analysis of Aikawa et al. (see paragraph 1 above), Applicants cannot identify any similarity or relation between the "encrypting conversion apparatus" described by Aikawa et al. and the system and method of the instant invention.

Moreover, as Applicants have concluded on their analysis of Aikawa et al. (see paragraphs 2 and 3 above), even when Aikawa et al. utilizes "*a module for dividing inputted plain-text data into first data and second data*", this procedure has no similarity with the procedure of *"splitting said original (or marked text document) into a first subset and a second subset of said words including the trailing said inter-word intervals of said words",* in the present invention. In fact, while in the present invention a complete input text (independently of its size) is pseudo-randomly split into two non contiguous portions or sub-texts, Aikawa et al. splits the input text for processing as a (fixed) sequence of contiguous blocks of 64 bits, where each 64 bits block is itself split into two contiguous sub-blocks of 32 bits each (left and right), denoted respectively: L[N] and R[N]. Thus, Applicants respectfully reject this assertion of the Examiner.

3) With respect to Claim 4 which states:

- - 4. The method ... wherein said authentication pattern, said blurring pattern and said splitting pattern are binary vectors comprised of a number of bits matching the number of corresponding said inter-word intervals. - -

The Examiner considers that the limitation of:

"*wherein said authentication pattern, said blurring pattern and said splitting pattern are binary vectors comprised of a number of bits matching the number of corresponding said inter-word intervals*".

is met by Aikawa, et al. column 10, lines 42-67 - Column 11, lines 1-67) which states:

In the instant embodiment of the invention, nine data mentioned below are used. L : data to undergo encrypting conversion (32 bits) R : data to undergo encrypting conversion (32 bits) KA : data of work key #1 (32 bits) KB : data of work key #1 (32 bits) KG : data of work key #2 (32 bits) Q : internal status value of cyclic shift generating module (8 bits) N : counter value (8 bits) X : data for the work (32 bits) S : data for the work (32 bits) Now, processing contents illustrated in FIG. 14 will be described in order. (1) In a processing step 1001 shown in FIG. 14, a plain-text C of 64bits is divided into more significant 32-bit data which are substituted for (or set as) the encrypting conversion undergoing data L and the encrypting conversion undergoing data R, respectively. (2) In a processing step 1002 shown in FIG. 14, a counter value N is set to "1". (3) In a processing step 1003 shown in FIG. 14, a returned value of an local variable initializing function INIT(KG, N) incorporated in the cyclic shift generating module is substituted for the internal status value Q of the cyclic shift generating module. In the case of the instant embodiment of the invention, the returned value of the local variable initializing function INIT(KG, N) incorporated in the cyclic shift is determined from the values of the work key (#2) KG{3N-3} and the work key (#2) KG{3N-2} in a processing step 1101 shown in FIG. 15. (4) Exclusive-OR of the encrypting conversion undergoing data L and the work key (#1) data KA is substituted for (or set as) the work-oriented data X in a processing step 1004 shown in FIG. 14. (5) In a processing step 1005 shown in FIG. 14, the returned value S=FUNC(X, KG, N, Q) from the cyclic shift and add function is added with "1" and is substituted for (or set as) the work-oriented data X. (6) In a processing step 1006 shown in FIG. 14, the returned value S=FUNC(X, KG, N, Q) from the cyclic shift and add function is substituted for the work-oriented data X. (7) The work-oriented data X is added with the work key (#1) KB data and substituted for the work-oriented data X in a processing step 1007 shown in FIG. 14. (8) In a processing step 1008 shown in FIG. 14, the returned value S=FUNC(X, KG, N, Q) from the cyclic shift and add function is

substituted for the work-oriented data X. (9) The work-oriented data X is added with the encrypting conversion undergoing data R and substituted for (or set as) the work-oriented data X in a processing step 1009 shown in FIG. 14. (10) The encrypting conversion undergoing data L is substituted for the encrypting conversion undergoing data R in a processing step 1010 shown in FIG. 14. (11) The work-oriented data X is substituted for the encrypting conversion undergoing data L in a processing step 1011 shown in FIG. 14. (12) In a processing step 1012 shown in FIG. 14, it is decided whether or not the counter value N is smaller than "10" inclusive. (13) When it is decided in the decision step 1012 that the counter value N is not greater than "10", then the value of the counter value N is incremented by "1" (one) in a processing step 1013 shown in FIG. 14. Subsequently, the processing step 1003 is resumed. (14) On the other hand, if the counter value N is greater than "10" in the step 1012, then the encrypting conversion undergoing data L is combined with the encrypting conversion undergoing data R, the result of which is outputted as an encrypted text M. The cyclic shift and the add function FUNC(X, KG, N, Q) are realized through the processions illustrated in a flow chart of FIG. 16. The contents of the processions shown in this figure will be described below. (1) On the basis of the internal status value Q, the leftward cyclic shift by 2 bits, by 8 bits or by 14bits is performed for the work-oriented data X, the result of which is saved as the work-oriented data S in a processing step 1201 shown in FIG. 16. (2) Result of the addition of the work-oriented data S and the work-oriented data X is again saved as the work-oriented data S in a processing step 1202. (3) In case the value of the work-key (#2) data KG{3N-1} is "0", the internal status value Q is updated to a value equal to a remainder resulting from division of the result of incrementation of the internal status value Q by "1", whereas when the value of the work key (#2) data KG{3N-1} is "1", the internal status value Q is updated to a value equal to a remainder resulting from division of the result of decrementation of the internal status value Q by "1" (processing step 1203 in FIG. 16). (4) The value of the work-oriented data S is substituted for the returned value in a processing step 1204 shown in FIG. 16.

From Applicants' analysis of Aikawa et al. (see paragraph 1 above) Applicants cannot identify any similarity, relationship or relevance between the "encrypting conversion apparatus" described by Aikawa et al. and the system and method of the instant invention. Applicants cannot identify in Aikawa et al. any item, concept or idea similar to the *"authentication patterns, blurring patterns and splitting patterns"* as that recited in this claim of the instant invention.

Moreover, confirming the conclusions of the analysis of Aikawa et al. (see paragraphs 2 and 3 above), the above paragraph states that in Aikawa: *"... a plain-text C of 64bits is divided into more significant 32-bit data which are substituted for (or set as) the encrypting conversion undergoing data L and the encrypting conversion undergoing data R, respectively"*. Observe that this procedure is absolutely different from and has no similarity with the procedure of the instant invention for generating *"said authentication pattern, said blurring pattern and said splitting pattern (as) binary vectors comprised of a number of bits matching the number of corresponding*

said inter-word intervals," that is implemented by the functional module depicted in Figure 2 of the instant application.

The Examiner has rejected (and is requested to reconsider the rejections of) Claim 1 under 35 U.S.C. 103(a) as being unpatentable over Bender (Techniques for Data Hiding) in view of Aikawa et al (US 6,606,385 B1).

In the rejection of Claim 1, the Examiner considers that the language found therein:

"*A method of marking an original text document, said original text document comprised of words separated by inter-word intervals, said inter-word intervals including one or more blank characters, said method consisting in altering the numbers of said blank characters, said method comprising the steps of: applying a reversible transform over said original text document in order that all said inter-word intervals become exclusively comprised of odd numbers of said blank characters*;

is met by Bender et al. on pages 332-333, in the "Open Space Methods" section.

The present invention utilizes an "open space" method to merge (under the form of extra inter-word blanks) the information necessary to authenticate a text document into the body of the document itself. This protocol is different from all "open space" methods disclosed in the prior art (Bender et al. included), in that the prior art merges the extra blanks, actually carrying the authentication data, with dummy blanks so as to confuse an attacker, while permitting the recipient of the document to restore exactly the format, including the number of blanks, of the original text.

In particular, the idea of *"applying a reversible transform over said original text document in order that all said inter-word intervals become exclusively comprised of odd numbers of said blank characters"* (Claim 1 herein) is absent in the "open space" methods described in Bender et al.. This step is an important contribution of the instant invention, since it has been purposely devised for providing "reversibility", i.e., permitting the recipient of a marked (authenticated) document to restore exactly the format, including the number of blanks, of the original text.

Thus, Applicants respectfully reject this assertion of the Examiner, since the above limitation cited in Claim 1 contains and combines inventive steps, not rendered obvious by the cited prior art.

Next, the Examiner concedes that Applicants' limitation of:

"splitting transformed said original text document into a first subset and a second subset of said words including the trailing said inter-word intervals of said words; and, over said first subset: computing, from said original text document and a secret-key , an authentication pattern that fits the number of said intervals of said first subset; adding inter-word blank characters in positions corresponding to said authentication pattern; generating canonical form of said first subset; computing, from said canonical form of said first subset and said secret-key, a blurring pattern that fits the number of said intervals of said first subset; modifying the numbers of inter-word blank characters according to said blurring pattern; and, over said second subset: generating canonical form of said second subset; computing, from said canonical form of said second subset and said secret-key, a blurring pattern that fits the number of said intervals of said second subset; modifying the numbers of inter-word blank characters according to said blurring pattern; recombining said first subset and said second subset thereby, obtaining a marked text for authentication."

is not met by Bender et al., but is met by Aikawa et al. at column 2, lines 42-65 which states:

"Thus, there is provided according to an aspect of the present invention an encrypting conversion apparatus which receives as inputs thereto at least one key and plain-text data to thereby output encrypted text data, which apparatus can be implemented in hardware fashion or software fashion and includes a cyclic shift processing module for determining a shift number on the basis of data for determining a shift number selecting sequence, a module for dividing inputted plain-text data into first data and second data and setting the first data as data L[1] while setting the second data as data R[1], at least one stage of an encrypting conversion processing module for receiving as inputs thereto data L[N] and R[N] to thereby output data L[N+1] and data R[N+1], wherein the encrypting conversion processing module is so arranged as to perform at least once for the data L[N] a conversion processing by using the key and a cyclic shift processing by means of the cyclic shift processing module, respectively, to thereby generate data X and wherein a value derived from arithmetic operation of the data R[N] and the data X is set as the data L[N+1] while the data L[N] being set as the data R[N+1], and a module for outputting a combination of two output data from a final stage of the encrypting conversion processing module as an encrypted text."

See Applicants analysis of Aikawa et al. (see paragraphs1, 2, 3, 4), on the above-paragraph cited by the Examiner. Applicants cannot identify any similarity or conceptual

relationship between the "*encrypting conversion apparatus which receives as inputs thereto at least one key and plain-text data to thereby output encrypted text data*" described by Aikawa et al. and the system and method of the instant invention.

The Examiner further supports this same rejection citing column 13, lines 13-26 which states:

"...Referring to the figure, a contents provider 1401 registers copyright information at a copyright managing facility 1418 to obtain contents identification information (IDA) 1402. The contents identification information (IDA) 1402 is embedded into the contents data 1403 by resorting to an electronic transparentizing technique (or so-called digital watermarking technique) which allows the identification information or the like to be contained in digital data in a hidden state, whereby package contents 1404 is finished. FIG. 19 is a schematic view illustrating the contents data contained in the package contents 1404, wherein the contents identification information (IDA) 1402 is embedded as an electronic transparent information..."

Applicants respectfully submit that the above-excerpt from Aikawa, et al. refers to a technique for hiding data (the IDA) on a format different from a plain text document (as for example, videos, music songs or digital pictures). Observe that, in the Bender, et al. reference cited by the Examiner, this watermarking technique cannot be applied for hiding data on plain text documents, as is the case of the operative environment of the instant invention.

In fact, according to Bender et al., page 332, *Data Hiding in Text* section, soft-copy texts are in many respects the most difficult places to hide (i.e., to steganographically hide) data. This is due mainly to the relatively small quantity of redundant information in a text file, as compared with an image or sound record. Although one can often imperceptibly modify a picture, this is not the case for a soft-copy text, where a single modification to the text, like an extra letter or period, can be noticed even by a casual reader. Hence, the argument on the cited paragraph can not properly be applied to the instant invention.

Referring also to column 13, lines 51-64, Aikawa, et al. state:

When the contents data is to be transferred from the personal computer (C) 1411 to the network, the user identification information (IDC) 1414 issued by the copyright managing facility 1418 is embedded in the contents data as the electronic transparent information in the personal computer

(C) 1411, whereon the contents data incorporating the electronic transparent information is encrypted with key data (K) 1415 by the encryption apparatus 1413 incarnating the teachings of the invention. FIG. 21 is a view showing schematically and illustratively the contents data transmitted along a path 1416, which contains the contents identification information (IDA) 1402, the user identification information (IDB) 1407 and the user identification information (IDC) 1414 as the electronic transparent information.

The Examiner states in the Official Action that : *"The IDA is the transparent, embedded watermark used for copyright protection."*

As Applicants have stated before, in the present invention, there is not any decryption process, since text documents are transmitted and received as plain (i.e., non-encrypted) text documents. Also, the above paragraph of Aikawa et al. refers to a technique for extracting from encrypted content data, data (the IDA) that has been encoded and hidden before encryption into content data having a format different than a plain text document (as for example, videos, music, or digital pictures) . Observe that, from the same reference cited by the Examiner (see Bender et al.), this "*transparentizing technique (or so-called digital watermarking technique)*" cannot be applied for hiding data on plain text documents, as is the case in the instant invention. In fact, according to Bender et al., page 332, *Data hiding in text section*, soft-copy texts are in many respects the most difficult places to hide (i.e., to steganographically hide) data. This is due mainly to the relatively small quantity of redundant information in a text file, as compared with an image or sound record. Although one can often imperceptibly modify a picture, this is not the case for a soft-copy text, where a single modification to the text, like an extra letter or period, can be noticed even by a casual reader. Hence, the argument on the excerpt cited by the Examiner ins upport of the rejection can not be properly applied to the instant invention.

Finally, the Examiner states that:

"It would have been obvious to one of ordinary skill in the art at the time the invention was made to generate the canonical form of each subset of data because this compress the data and hence reduces the amount of overhead being sent when the watermarked text document is transmitted from a sender to a receiver."

As discussed in the analysis of Aikawa et al. (see paragraph 4 above), on the system of Applicants' invention, "canonical forms" of texts are purposely and exclusively used to generate "authentication patterns, blurring patterns and splitting patterns," not to compress the data to be transmitted. In fact, in Applicants' invention, the "canonical form" of a text is only used for computation purposes, and never is transmitted. Thus, Applicants respectfully reject this assertion of the Examiner.

The Examiner rejects (and is requested to reconsider such rejection of) Claims 5, 6, 7 and 8 under 35 U.S.C. 103(a) as being unpatentable over Aikawa et al (US 6,606,385 B1) in view of Bender (Techniques for Data Hiding).

With respect to Claim 5:

5. *The method ... wherein said canonical form is obtained in stripping all blank characters, in excess of one, off said inter-word intervals.*

The Examiner considers that Aikawa et al. meets all the limitation except for the following limitation :

"*wherein said canonical form is obtained in stripping all blank characters, in excess of one, off said inter-word intervals*".

The Examiner asserts that this missing element is disclosed by Bender on pages 3332 and 333, in the "Open Space Methods" section.

In their analysis of Aikawa et al. (see paragraph 4), and Bender et al., Applicants have established that the concept of the "canonical form" of a text document is exclusively found in Applicants' invention. Neither reference cited, alone or in combination discloses the elements of

the claims and there is no basis for combination of the cited references as they teach in opposite directions.

The Examiner also contends that:

"It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bender within the system of Aikawa et al because stripping all the blank characters in excess of one character manipulates the white space manipulation to achieve data compression. This saves overhead during data transmission".

Applicants demonstrated in their analysis of Aikawa et al. (see paragraph 4) and of Bender et al., in the system of the present invention that "canonical forms" of texts are purposely and exclusively used to generate "authentication patterns, blurring patterns and splitting patterns", concepts which are unique to the present invention, and are not used to compress the data to be transmitted. In fact, in the present invention the "canonical form" of a text is exclusively used for computational purposes, to generate those patterns, and never is transmitted.

6) With respect to Claim 6:

6. The method ... wherein modifying steps include:
in the positions corresponding to the asserted bits of said blurring patterning one blank character if said inter-word intervals are comprised of an odd number of said blank characters;
removing one blank character if said inter-word intervals are comprised of an even number of said blank characters.

The Examiner in the Official Action asserts that Aikawa et al. meets all the limitations of Claim 6, except for the following limitation which is listed as follows:

"*wherein modifying steps include: in the positions corresponding to the asserted bits of said blurring patterns: adding one blank character if said inter-word intervals are comprised of an odd number of said blank characters; removing one blank character if said inter-word intervals are comprised of an even number of said blank characters*" which is of course the entire wording of Claim 6.

The Examiner considers that this element is fulfilled by Bender on pages 3332 and 333, in the "Open Space Methods" section.

From their analysis of Aikawa et al. (see paragraph 4), and Bender et al., Applicants have concluded that the generation and use of "blurring patterns", selectively applied to inter-words blanks intervals of a text document, is exclusive to their invention. Applicants cannot identify nor has the Examiner adequately demonstrated a similar concept or function in the two references cited.

The Examiner also considers that:

"*It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bender within the system of Aikawa et al because stripping all the blank characters in excess of one character manipulates the white space manipulation to achieve data compression. This saves overhead during data transmission*".

As noted in the above-noted analysis of Aikawa et al. (see paragraph 4) and of Bender et al., in considering the system of Applicants invention, "canonical forms" of texts are purposely and exclusively used to generate "authentication patterns, blurring patterns and splitting patterns", and not to compress the data to be transmitted. Thus, Applicants respectfully reject this assertion of the Examiner.

7) With respect to Claim 7:

7. "The method ... wherein modifying steps and erasing steps perform identically."

The Examiner considers that the limitation of:

"wherein modifying steps and erasing steps perform identically" is met in Aikawa, et al. at Column 3, lines 11-33 which states:

Further, according to another aspect of the present invention, there is provided a decrypting conversion apparatus which receives as inputs thereto at least one key and encrypted text data to thereby output plain-text data, which apparatus can be implemented hardware-wise or softwarewise and includes a cyclic shift processing module for determining a shift number on the basis of data for determining a shift number selecting sequence, a module for dividing inputted encrypted text data into first data and second data and setting the first data as data L[1] while setting the second data as data R[1], at least one stage of a decrypting conversion module for receiving as inputs thereto data L[N] and R[N] to thereby output data L[N+1] and data R[N+1], wherein the decrypting conversion module is so arranged as to perform at least once for the data R[N] a conversion processing by using the key and a cyclic shift processing by means of the cyclic shift processing module, respectively, to thereby generate data X and wherein a value derived from arithmetic operation of the data L[N] and the data X is set as the data R[N+1] while the data R[N] being set as the data L[N+1], and a module for outputting a combination of two output data from final stage of the encrypting conversion module as a plain-text.

Based upon their analysis of Aikawa et al. (see pargraphs 1, 2, 3, 4) on the above paragraph cited by the Examiner, Applicants cannot identify, nor has the Examoiner demonstrated, any similarity or proper relationship between this "decrypting conversion apparatus" described by Aikawa et al. and the system and method of the present invention. The "modifying steps and erasing steps" subject of the instant Claim 7 relate to the generation of "authentication patterns, blurring patterns and splitting patterns", concepts which are original and exclusive to the present invention, and are missing in the references, alone and in combination, cited by the Examiner.

8) With respect to Claim 8:

8. "The method according to...wherein extracting step includes:

removing one blank character in those of said inter-word intervals that are comprised of an even number of said blank characters;

obtaining a binary authentication vector with asserted bits corresponding to positions where said blank characters were removed.

The Examiner asserts that Aikawa, et al meets all the limitations, except for the following limitation :

"*wherein extracting step includes: removing one blank character in those of said inter-word intervals that are comprised of an even number of said blank characters; obtaining a binary authentication vector with asserted bits corresponding to positions where said blank characters were removed,*"

which the Examiner considers is disclosed by Bender on pages 332 and 333, in the "Open Space Methods" section.

Applicants do not disclose any "extracting step" (of blank characters from a text document), or any similar concept in Aikawa et al. (see arguments in paragraphs 1, 2, 3, 4). Also, from their analysis of Bender et al. Applicants cannot identify in the section dedicated to describe "open space methods" (or on any other section of this reference), anything similar to the procedure subject of Claim 8 of the instant invention.

The Examiner also considers that:

"It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Bender within the system of Aikawa et al because stripping all the blank characters in excess of one character manipulates the white space manipulation to achieve data compression. This saves overhead during data transmission".

The "extracting step" subject of Claim 8 (dependent on the authentication method of Claim 2) is performed, after an authenticated document has been received, for the purpose of "obtaining a binary authentication vector" (i.e., the MAC or digital signature) encoded inside by the sender. Thus, this "extracting step" is aimed exclusively for the purposes of authentication of the received document, and not for the purposes of data compression, to save storage, or for saving overhead during data transmission. Therefore, Applicants respectfully oppose this assertion by the Examiner.

In conclusion, the Applicant respectfully reject the Examiner's objections. There is absolutely no showing or suggestion in prior art of a system such as that described and expressly claimed within the present application.

Applicants, in their conclusion wish to emphasize that the prior art references cited are directed to "encryption" systems whereas their invention, as noted above, is, *inter alia,* directed to steganographic data hiding techniques. As is known, steganography is the concealment of a small message inside a larger file that appears to consist entirely of something else. Steganography goes hand-in-hand with encryption, but is not the same thing. Encryption makes a message unreadable by unauthorized persons; steganography hides the very existence of the message. This contrast is at the heart of the application for Letters Patent. The prior art relates to encryption and Applicants invention relates to steganography. The there is patentable subject matter in the instant application.

Applicants hereby request a one month extension of time within which to file this amendment. A check in the amount of $110.00 is enclosed to cover the extension fee.

In view of the above, Applicants respectfully request allowance of the claims.

Respectfully Submitted,

Thomas A. Beck
26 Rockledge Lane
New Milford, CT 06776
Telephone (860) 354-0892

I hereby certify that this paper is being deposited on the date indicated below with the U.S. Postal Service as First Class Mail addressed to Commissioner of Patents & Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

January 12, 2005

Name: Thomas A. Beck

APPENDIX

1. (Original) A method of marking an original text document,

said original text document comprising words separated by inter-word intervals, said inter-word intervals including one or more blank characters having numbers, said numbers being altered, said method of altering said numbers of said blank characters, comprising the steps of:

applying a reversible transform over said original text document in order that all said inter-word intervals become exclusively comprised of odd numbers of said blank characters;

splitting and transforming said original text document into a first subset and a second subset of said words including trailing blanks of said inter-word intervals of said words;

and, over said first subset:

computing from said original text document and a secret-key, an authentication pattern that fits the number of said intervals of said first subset;

adding inter-word blank characters in positions corresponding to said authentication pattern;

generating a canonical form of said first subset;

computing, from said canonical form of said first subset and said secret-key, a blurring pattern that fits the number of said intervals of said first subset;

modifying the numbers of inter-word blank characters according to said blurring pattern;

and, over said second subset:

generating canonical form of said second subset;

computing, from said canonical form of said second subset and said secret-key, a blurring pattern that fits the number of said intervals of said second subset;

modifying the numbers of inter-word blank characters according to said blurring pattern;recombining said first subset and said second subset thereby, obtaining a marked text for authentication.

2. (Original) A method of authenticating a marked text document, said marked text document comprising words separated by inter-word intervals, said inter-word intervals including one or more blank characters having numbers which are checked, said method comprising checking the numbers of said blank characters utilizing the steps of:

splitting said marked text document into a first subset and a second subset of said words including trailing blanks of said inter-word intervals of said words; and,

over said first subset:

generating a canonical form of said first subset;

computing from said canonical form of said first subset and a secret-key

a blurring pattern that fits the number of said intervals of said first subset;

erasing modifications brought to the numbers of said inter-word blank characters per said blurring pattern;

extracting an authentication pattern thereby,

obtaining in all said inter-word intervals, odd numbers of blank characters; and,

over said second subset:

generating canonical form of said second subset;

computing from said canonical form of said second subset and said secret-key

a blurring pattern that fits the number of said intervals of said second subset;

erasing modifications brought to the numbers of said inter-word blank characters per said blurring pattern thereby, obtaining in all said inter-word intervals,

odd numbers of blank characters ;

recombining said first subset and said second subset;

applying a reverse transform thus retrieving said original text document;

computing from retrieved, said original text document and said secret-key an authentication pattern that fits the number of said intervals of retrieved said original text document ;

comparing extracted said authentication pattern and computed said authentication pattern;

if matching exactly, accepting said marked text document as authentic;

if not:

rejecting said marked text document as fake.

3. (Original) The method defined in claim 2 wherein splitting steps includes the preliminary steps of generating a canonical form of a text document; computing, from said canonical form of said text document and said secret-key, a splitting pattern that fits the number of said intervals of said text document; thereby, allowing to split and to recombine said text document on the basis of asserted and non-asserted bits of said splitting pattern.

4. (Original) The method defined in claim 3 wherein said authentication pattern, said blurring pattern and said splitting pattern are binary vectors comprising a number of bits matching the number of said inter-word intervals.

5. (Original) The method defined in claim 4 wherein said canonical form is obtained in stripping all blank characters, in excess of one, off said inter-word intervals.

6. (Original) The method defined in claim 5 wherein modifying steps include:
in the positions corresponding to the asserted bits of said blurring patterns:
adding one blank character if said inter-word intervals comprise of an odd number of said blank characters; and
removing one blank character if said inter-word intervals comprise an even number of said blank characters.

7. (Original) The method defined in claim 6 wherein modifying steps and erasing steps are performed identically.

8. (Original) The method defined in claim 7 wherein extracting step includes removing one blank character in those of said inter-word intervals that are comprised of an even number of said blank characters;
obtaining a binary authentication vector with asserted bits corresponding to positions where said blank characters were removed.